Emerging Trends in Fraud and Anti-Money Laundering

The changing landscape of Fraud and AML enforcement
Objectives:

1. Identify six emerging trends of fraud and AML enforcement
2. Look at the growth rate of these trends
3. Understand the typologies of those trends
4. What are the behavioral and transactional red flags in each of these areas
5. What are your role and responsibilities in fraud and AML enforcement
Six Emerging Fraud and AML Trends

1. Cannibus Banking
2. Financial Exploitation of the Elderly (FEEVA)
3. Cryptocurrency
4. Peer to Peer Transactions (P2P)
5. Human Trafficking
6. Online Gambling
Emerging Fraud and AML Trends - Identified

➡️ CANNIBUS BANKING
- Cheech and Chong’s “Up in Smoke” (1978).
Cannibus Banking: What is the problem???
Cannibus Banking – From criminality to commercial enterprise

As of October 2018, 30 states and the District of Columbia have legalized marijuana for medical use, nine states and the D.C. have legalized it for recreational use, and 22 states and the District of Columbia have decriminalized it.

1. Confusion due to different levels of legalization by state (none, medical, fully permitted)
2. Marijuana is still banned as a controlled substance as a Schedule 1 drug at the federal level.
3. Marijuana related businesses (MRB) fall into one of 3 tiers:
   - Tier 1: Touch the plant companies
   - Tier 2: Service providers for Tier 1
   - Tier 3: Companies that happen to serve Tier 1 or 2.
4. FinCen special due diligence for MRB's is a good guide. (Only applicable to MRB's in states that are legal.)
Banking Due Diligence over MRBs

- FinCEN special due diligence for MRBs that are legal under state law:
  1. Is the company licensed?
  2. Review of the licensure application.
  3. Request info about the applicants from the state regulators.
  4. Develop an understanding of normal and expected activities of the customer.
  5. Ongoing monitoring of publicly available sources for adverse info about the business and related parties.
  6. Ongoing monitoring for suspicious activity.
  7. Periodically refreshing info obtained during CDD, commensurate with risk.
Possible Banking MRB Activities

1. A bank wants to serve as a securities custodian for a private equity fund. Private equity fund would only invest in companies that are operating legally under state law.

2. A bank is financing the mortgage on a condo used by a licensed physician with dispensing privileges. Loan agreement has a criminal activities/CSA clause in it.

3. A bank finances the purchase of agricultural land that is being used for growing marijuana in a legal state.

4. A private equity company assists a grower/dispensary in raising investment capital.

5. A bank provides a working capital line of credit to an accounting firm that has a number of legal marijuana businesses as clients.

6. A bank has extended a 5-year line of credit to a dispensary in a legal state, then one year into the loan, the dispensary loses its license.
1. A bank provides a loan to a company located in a state where marijuana is not legal. The company manufacturers marijuana equipment in that state then sends it to legal states for sale.

2. A bank is asked to provide a loan to a dispensary operating legally in a state, but learns that the CEO has a prior fraud conviction in connection with an unrelated legal enterprise.

3. A bank has a deposit account to a corporate customer in a legal state. An corporate affiliate of the corporate customer located in another state is charged by the DOJ with money laundering.

4. The bank is acting as trustee on a trust for the benefit of a child with a serious illness that can be treated with cannabis. The child’s guardian requests disbursement to a medical marijuana company for the purchase of legal marijuana.
What to do?

“Probably the best advice we could give is that if you are a bank and you have marijuana-related businesses as customers, you should follow that FinCEN guidance, because I think that would help to protect you.”

- OCC Deputy Chief Counsel during a panel presentation (2014).

Regarding the FinCEN policy: “We are reviewing it, but the intent is not to take it down without a replacement that can deal with the current situation . . . . We want to make sure that we can collect our necessary taxes and other things.”

- Treasury Secretary Steven Mnuchin, Feb. 6, 2018, Testimony Before the House Financial Services Committee.
Emerging Fraud and AML Trends - Identified

» FINANCIAL EXPLOITATION OF THE ELDERLY (FEEVA)
FEEVA Defined:

- Financial exploitation occurs when a person misuses or takes the assets of a vulnerable adult for his/her own personal benefit. This frequently occurs without the explicit knowledge or consent of a senior or disabled adult, depriving him/her of vital financial resources for his/her personal needs.

- Assets are commonly taken via forms of deception, false pretenses, coercion, harassment, duress and threats.
What FEEVA looks like?

- Growing due to aging baby boomer population.
- 90% of FEEVA cases contain the following characteristics:
  - Isolation vulnerability of the victim
  - Children of elderly
  - In home health care workers - access to banking data
  - Romance scams
  - Internet and phone scams (increased use of phishing)
Consumer Financial Protection Bureau indicates a quadruple increase of reported cases from 2013 – 2017 and is still increasing.

Only a fraction of the 3.5 million of incidences of financial elder exploitation.

Over the last 3 years, an estimated $6 billion was taken from individuals over the age 70.

Average loss per reported incident has increased to $50,000.
Common Forms of Financial Exploitation

- **Theft**: involves assets taken without knowledge, consent or authorization; may include taking of cash, valuables, medications other personal property.

- **Fraud**: involves acts of dishonestly by persons entrusted to manage assets but appropriate assets for unintended uses; may include falsification of records, forgeries, unauthorized check-writing, and Ponzi-type financial schemes.

- **Real Estate**: involves unauthorized sales, transfers or changes to property title(s); may include unauthorized or invalid changes to estate documents.

- **Contractor**: includes building contractors or handymen who receive payment(s) for building repairs, but fail to initiate or complete project; may include invalid liens by contractors.

- **Lottery scams**: involves payments (or transfer of funds) to collect unclaimed property or “prizes” from lotteries or sweepstakes.
Common Forms of Financial Exploitation (Cont.)

- **Electronic**: includes “phishing” e-mail messages to trick persons into unwittingly surrendering bank passwords; may include faxes, wire transfers, telephonic communications.

- **Mortgage**: includes financial products which are unaffordable or out-of-compliance with regulatory requirements; may include loans issued against property by unauthorized parties.

- **Investment**: includes investments made without knowledge or consent; may include high-fee funds (front or back-loaded) or excessive trading activity to generate commissions for financial advisors.

- **Insurance**: involves sales of inappropriate products, such as a thirty-year annuity for a very elderly person; may include unauthorized trading of life insurance policies.
The key to spotting financial abuse is a change in a person’s established financial patterns.

Watch out for these red flags:

1. Unusual activity in an older person’s bank accounts, including large, frequent or unexplained withdrawals.
2. Changing from a basic account to one that offers more complicated services the customer does not fully understand or need.
3. Withdrawals from bank accounts or transfers between accounts the customer cannot explain.
5. Sudden non-sufficient fund activity or unpaid bills.
6. Closing CDs or accounts without regard to penalties.
Red Flags for Elder Financial Abuse (Cont.)

- 7. Uncharacteristic attempts to wire large sums of money.
- 8. Suspicious signatures on checks, or outright forgery.
- 9. Confusion, fear or lack of awareness on the part of an older customer.
- 10. Checks written as “loans” or “gifts”.
- 11. Bank statements that no longer go to the customer’s home.
- 12. New powers of attorney the older person does not understand.
- 13. A caretaker, relative or friend who suddenly begins conducting financial transactions on behalf of an older person without proper documentation.
Emerging Fraud and AML Trends - Identified

- Cryptocurrency
Cryptocurrency Defined:

- A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems.

- The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.
Cryptocurrency Emergence

- Industry experts view cryptocurrency as the next wave of financial exchange and the fastest growing financial exchange medium since credit cards were introduced in the 1950's. (American Express)

- Currently it appears that cryptocurrency is being used for investment purposes due to the rapid increase in value.

- Use of cryptocurrency as a financial exchange medium appears to in its infancy stages and currently has more viability in the dark web activities.

- Once cryptocurrency becomes main stream and widely excepted, AML and fraud enforcement issues will skyrocket.
Strengths of Cryptocurrency

1. Scalable
2. Exchangeability
3. Security
4. Speed of transactions
5. Low Transaction Fees
6. Transparency
7. Scarcity
8. Less risk to merchants
Weaknesses of Cryptocurrency

1. Unfriendly regulatory environment

2. Price fluctuation vs U.S. dollar

3. Increase of attacks on cryptocurrency system resulting in millions of dollars of losses
Cryptocurrency Risks

- Concerns abound that altcoins may become tools for anonymous web criminals. Used as a common exchange medium on the dark web.

- Cryptocurrency networks display a lack of regulation that has been criticized as enabling criminals who seek to evade taxes and launder money.

- Transactions that occur through the use and exchange of these altcoins are independent from formal banking systems, and therefore can make tax evasion simpler for individuals due to the difficulty in tracking.

- Laundering money through altcoins can be achieved through anonymous transactions.
Cryptocurrency Flags

- Large cash deposits followed by ACH debits to cryptocurrency institutions like Bitcoin.
- ACH credits from traditional investment brokerage houses followed by ACH debits to Bitcoin.
- ACH credits from cryptocurrency institutions like Bitcoin and others.
- ACH debit or credit activity timed with the rise or fall of market value of Bitcoin and others.
- Customer due diligence identifying customer involved with cryptocurrency data mining.
Emerging Fraud and AML Trends - Identified

Peer to Peer (P2P) Transactions
Peer to Peer Systems Defined:

- **Peer-to-peer transactions** (also referred to as person-to-person transactions, P2P transactions, or P2P payments) are electronic money transfers made from one person to another through an intermediary, typically referred to as a P2P payment application.
Peer to Peer Ease of Use:

- P2P payments can be sent and received via mobile device or any home computer with access to the Internet, offering a convenient alternative to traditional payment methods.

- Smartphone technology affected many aspects of modern day life, one of those being the ability to transfer money to other people anywhere in the world within seconds. These apps allow users to easily send and receive payments in a short time frame, with little to no fees involved. The prevalence of smartphones allows most people to use their phones as a type of wallet, particularly when splitting bills or dealing with personal debts.
Peer to Peer Systems identified:

- Paypal, Venmo, Zelle, Square Cash are growing quickly and are the predominant P2P systems in use currently.

- Independent P2P payment systems (Paypal, Venmo (owned by Paypal), and Square Cash) exist outside of formal banking channels and have little to no oversight from the regulated institutions.

- Zelle is a bank-managed P2P system which inherently contains more granular oversight and regulation.
Peer to Peer Systems Emergence

All P2P Transactions: 2016 - $147B in transfers; projected 2020 $316B in transfers
P2P Flags: What to look for?

- Rapid movement of funds from Person A to Persons B, C, D and others and in reverse using P2P systems.
- International ACH credits followed by P2P payments to a network of individuals.
- Cash deposits followed by P2P payments to non-customers.
- P2P credits followed by cash withdrawals.
Emerging Fraud and AML Trends - Identified

► Human Trafficking
Human Trafficking Defined:

The Legal Definition of Human Trafficking

**Sex Trafficking**
The recruitment, harboring, transportation, provision, obtaining, patronizing, soliciting, or advertising of a person for a commercial sex act, in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years of age.

**Labor Trafficking**
The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.
Human Trafficking Emerging

1. Worldwide profits exceed $150 billion/year and growing.

2. Is still the globe's fastest growing crime despite increased awareness because it combines high profit and low risk.
Human Trafficking Red Flags

Transactional Indicators

• Numerous debit cards for a single personal account
  o Trafficker will often have victims working simultaneously in numerous locations.

• ATM cash deposits below threshold from locations other than where the account is domiciled
  o Victims are often required to deposit their profits daily into trafficker’s account.

• Frequent taxi/car service charges
• Frequent hotel charges
• Exploitive recruitment fees collected by labor agencies, brokers and other intermediaries in the victim’s home country
Face-to-Face Indicators (Branch Activity)

- Behavior/Roles of individuals during account opening
  - Does it appear that someone is in a controlling position?
  - Does someone have possession over the account holder’s identification documents?
  - Does someone speak for the account holder?
  - Does the account holder refuse to make eye contact with you?
- Cash deposits in small bills with an immediate transfer to a foreign country
  - Possibly a payment to trafficker or a debt payment.
- Business account holder cashing payroll checks
  - Good indicator that employees are without proper identification documents.
Internal Steps Banking Institutions can take to identify Human Trafficking

- Focus data mining on specific business sectors such as night clubs, spas, and employment agencies
- Initiate targeted reviews based on various sources such as negative news, published indicators, LE information, and typologies.
- Identify financial products exploited to facilitate the movement of funds and employ data mining (ie credit cards, ATMs and wire transfers)
- Educate first line personnel and staff about potential "face to face" indicators.
Emerging Fraud and AML Trends - Identified

- Online Gambling
Online Gambling Emerging – Projected Growth

Estimated U.S. Revenues:
2018 - $405 million
2019 - $648 million
2020 - $1.4 - $2.1 billion
2023 - $3.1 - $5.2 billion
Online Gambling Emerging

- 2018 Supreme Court decision to legalize sports betting is leading more states to legalize online gambling.

- At least 43 of 50 states offer at least one of the following online gambling products:
  - Sports Betting
  - Casino
  - Poker
  - Lottery
  - Horseracing
  - Daily Fantasy Sports
Online Gambling Emerging - Ohio

What about Ohio as of today?

- Sports Betting - No
- Casino - No
- Poker - No
- Lottery - No
- Horseracing - Yes
- Daily Fantasy Sports – Yes
Online Gambling Red Flags – Back Office

- Increase in unexplained wealth for customer.
- Account credits from an unknown payment processor service inconsistent with customer business type or customer explanation.
- Frequent unexplained wire transfers received and immediately withdrawn in cash.
- Credit card payments, bank transfers, etc. to mixed gambling chains like land-based casinos, betting shops, and other venues.
- ACH debit and credit activity from non-domestic and offshore gambling sites.
- Transfers between different customer accounts.
- Multiple accounts to accommodate mixed gambling chains.
Online Gambling Red Flags – Customer Facing

- Request by customer to wire funds to a stranger.
- Customer indicates an unidentified relative in crisis who needs wire funds.
- Customer states that a wire or ACH debit is the only payment form acceptable.
- Customer requests multiple account openings in the same name.
- Customer makes frequent cash withdrawals immediately after receiving ACH credits or incoming wires.
Online Gambling – Monitoring

- Bulk of responsibility will fall to the online gambling operators to become more efficient and accurate regarding the onboarding of new players to help mitigate risk.
- Banking KYC will become critical to properly identify the customer expected activity. Aggressive transaction monitoring should be bounced against expected gaming activity to determine risk behavior.
Emerging Trends in Fraud and Anti-Money Laundering

Jim Hixenbaugh
PNC Detection and Investigation Manager
440-376-7589
James.Hixenbaugh@pnc.com